



SPYWOLF

Security Audit Report



Completed on
March 10, 2023

@SPYWOLFNETWORK



@SPYWOLFNETWORK



SPYWOLF.CO





OVERVIEW

This audit has been prepared for **TOKERR** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

“

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

”





TABLE OF CONTENTS

Project Description	01
Contract Information	02
Current Stats	03
Vulnerability Check	04
Threat Levels	05
Found Threats	06-A/06-D
Good Practices	07
Tokenomics	08
Team Information	09
Website Analysis	10
Social Media & Online Presence	11
About SPYWOLF	12
Disclaimer	13



TOKERR



TOKERR

PROJECT DESCRIPTION

According to their whitepaper:

Tokerr is comprehensive ecosystem designed to make DeFi safe and accessible for investors and developers, by building innovative solutions to existing DeFi problems. The goal is to give users of Tokerr products access to an environment which they can invest with peace of mind and the knowledge that their investments are safe.

Release Date: Launched March 08, 2023

Category: DeFi / Bridge



CONTRACT INFO

Token Name
Tokerr

Symbol
TOKR

Contract Address

0xA885B6d3C87535de688194Ec3645199ee76D6772

Network
Ethereum

Language
Solidity

Deployment Date
March 08, 2023

Verified?
Yes

Total Supply
1,000,000

Status
Launched

TAXES

Buy Tax
4%

Sell Tax
4%

*Fees can be changed in future



Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



TOKEN TRANSFERS STATS

Transfer Count	511
Uniq Senders	64
Uniq Receivers	250
Total Amount	3136395.217097115 TOKR
Median Transfer Amount	722.6 TOKR
Average Transfer Amount	6137.759720346605 TOKR
First transfer date	2023-03-08
Last transfer date	2023-03-10
Days token transferred	3

SMART CONTRACT STATS

Calls Count	899
External calls	100
Internal calls	799
Transactions count	252
Uniq Callers	95
Days contract called	3
Last transaction time	2023-03-10 01:30:11 UTC
Created	2023-03-08 00:01:23 UTC
Create TX	0x35d94f8ac99bafc02581fee764cef7fb9ba98881c06f5f1f629b225afaf1b673
Creator	0xfac30a6539bcd57636a74c20b877ffd06c3929fa



VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed



THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

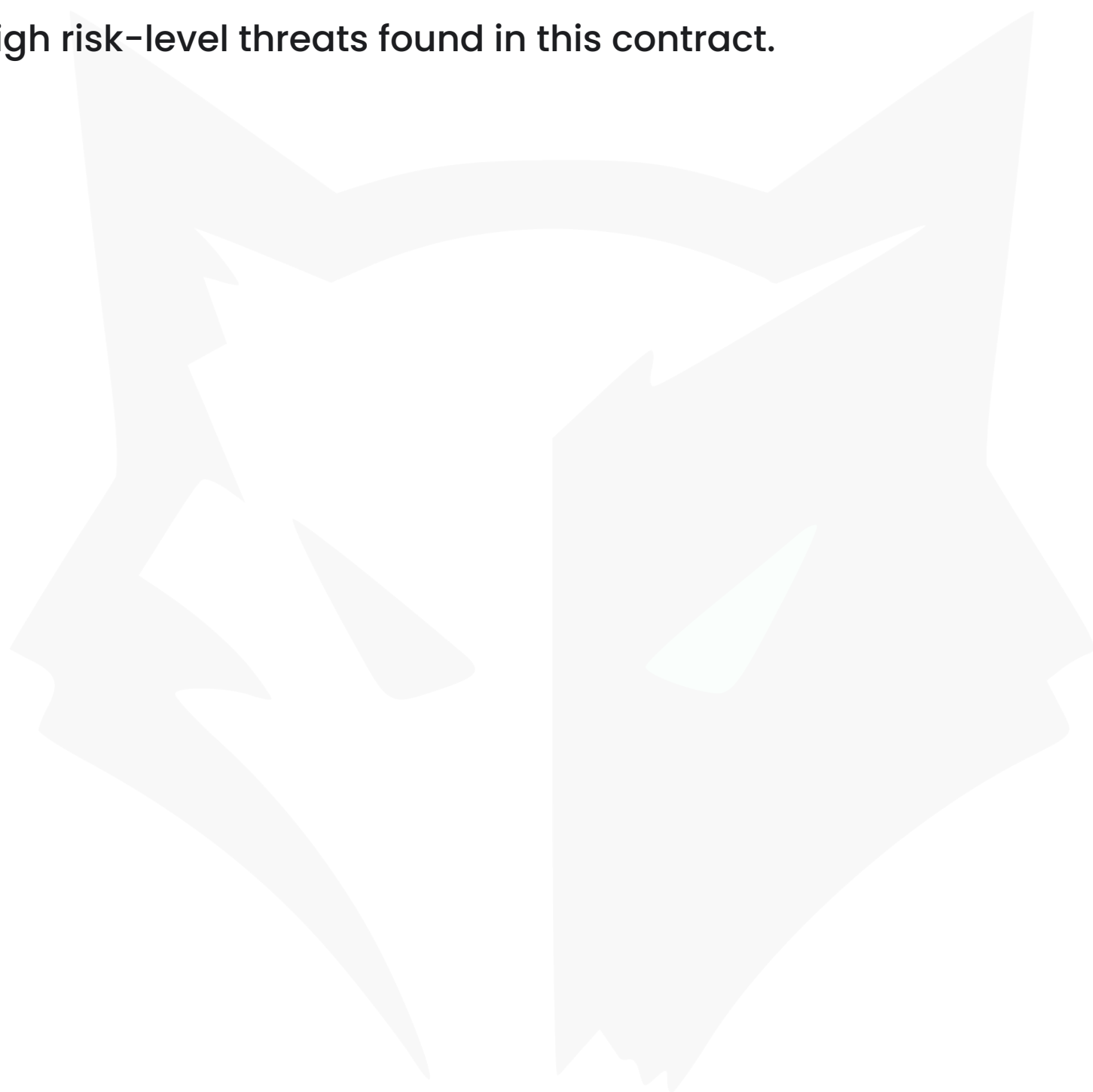
Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.



FOUND THREATS

High Risk

No high risk-level threats found in this contract.





FOUND THREATS

Medium Risk

Owner can change contract accumulated fees autoSwap criteria. If swapThreshold and/or swapRatio are set to 0 contract will halt and selling will fail.

```
function setTokenSwapSettings(bool _enabled, uint256 _threshold, uint256 _ratio, bool ratio) external authorized {
    swapEnabled = _enabled;
    swapThreshold = _threshold * (10 ** _decimals);
    swapRatio = _ratio;
    ratioSell = ratio;
}

function _transferFrom(address sender, address recipient, uint256 amount) internal returns (bool) {
    .....
    if(shouldTokenSwap(amount, recipient)){ tokenSwap(amount); }
    .....
}

function tokenSwap(uint256 _amount) internal swapping {
    uint256 amount = (ratioSell) ? _amount.mul(swapRatio).div(100) : swapThreshold;

    (amount > swapThreshold) ? amount : amount = swapThreshold;
    .....
}
```



FOUND THREATS

⚠ Low Risk

Owner can set buy/sell fees up to 15%.

Combined buy+sell=30%.

When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make.

Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```
function setBuyFees(uint256 _marketingFee, uint256 _liquidityFee,
    uint256 _teamFee) external authorized{
    require((_marketingFee.add(_liquidityFee).add(_teamFee)) <= 150);
    marketingBuyFee = _marketingFee;
    liquidityBuyFee = _liquidityFee;
    teamBuyFee = _teamFee;

    marketingFee = marketingSellFee.add(_marketingFee);
    liquidityFee = liquiditySellFee.add(_liquidityFee);
    teamFee = teamSellFee.add(_teamFee);

    totalBuyFee = _marketingFee.add(_liquidityFee).add(_teamFee);
    totalFee = liquidityFee.add(marketingFee).add(teamFee);
}

function setSellFees(uint256 _marketingFee, uint256 _liquidityFee,
    uint256 _teamFee) external authorized{
    require((_marketingFee.add(_liquidityFee).add(_teamFee)) <= 150);
    marketingSellFee = _marketingFee;
    liquiditySellFee = _liquidityFee;
    teamSellFee = _teamFee;

    marketingFee = marketingBuyFee.add(_marketingFee);
    liquidityFee = liquidityBuyFee.add(_liquidityFee);
    teamFee = teamBuyFee.add(_teamFee);

    totalSellFee = _marketingFee.add(_liquidityFee).add(_teamFee);
    totalFee = liquidityFee.add(marketingFee).add(teamFee);
}
```



Informational

Owner can change max transaction amount but cannot lower it than 1% of total supply.

When such restrictions are in place, the users can transfer token amounts up to said restriction value.

```
function setTxLimit(uint256 percent) external authorized {  
    require(percent >= 10); //1% of supply, no lower  
    _maxTxAmount = ( _totalSupply * percent ) / 1000;  
}
```

Eth can be withdrwn from the contract.

Withdrawn ether goes to the current marketingWallet.

When such function is present in the contract, accumulated ETH from sells of tokens from taxes can be withdrawn.

```
function clearStuckBalance() external {  
    uint256 amountETH = address(this).balance;  
    (bool tmpSuccess,) = payable(marketingWallet).call{value: amountETH, gas: 100000}("");  
    tmpSuccess = false;  
}
```



RECOMMENDATIONS FOR

GOOD PRACTICES

1

Consider fundamental tradeoffs

2

Be attentive to blockchain properties

3

Ensure careful rollouts

4

Keep contracts simple

5

Stay up to date and track development

Tokerr

GOOD PRACTICES FOUND

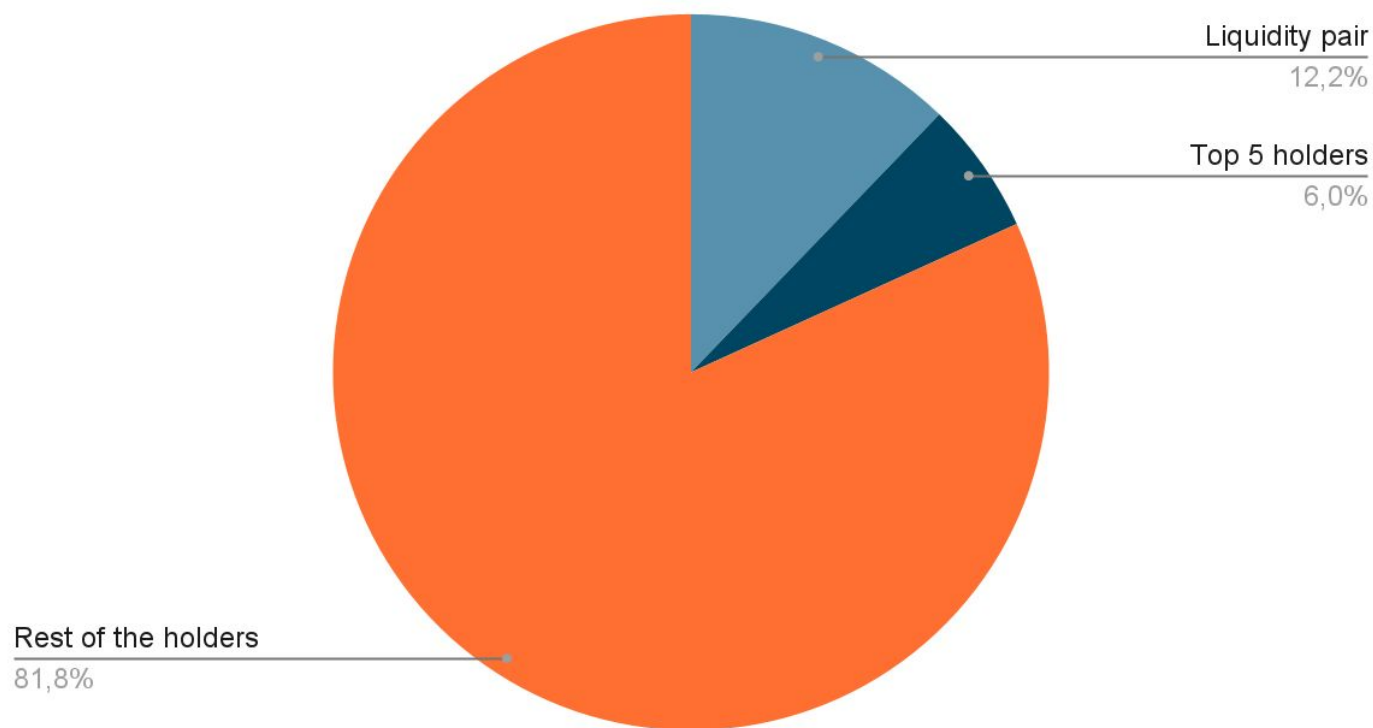
- ✓ The owner can set a transaction limit, but can't lower it than 1% of total supply
- ✓ The smart contract utilizes "SafeMath" to prevent overflows



Current tokens distribution according to Etherscan:

- 12.2% - Liquidity Pair
- 81.8% - Rest of the holders
- 6% - Top 5 holders

Tokens distribution





THE TEAM

! The team is anonymous

KYC INFORMATION

! No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.





WEBSITE

Website URL

<https://www.tokerr.io/>

Domain Registry

<https://www.godaddy.com>

Domain Expiration

Expires on 2023-08-26

Technical SEO Test

Passed

Security Test

Passed. SSL certificate present

Design

Nice overall design with appropriate color scheme and graphics.

Content

The information helps new investors understand what the product does right away. No grammar errors found. .

Whitepaper

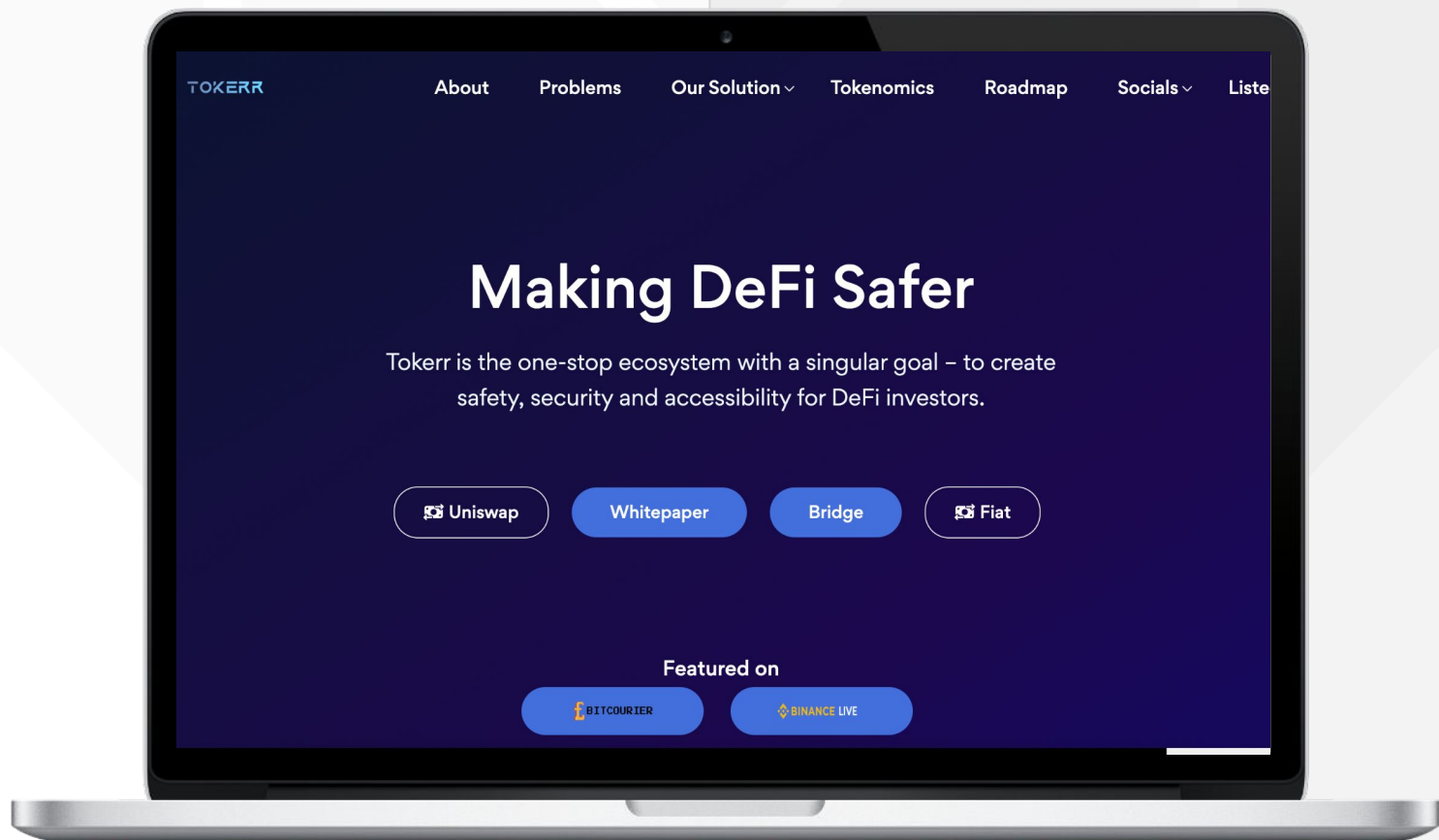
Well written, explanatory.

Roadmap

Yes, goals set without time frames.

Mobile-friendly?

Yes



tokerr.io



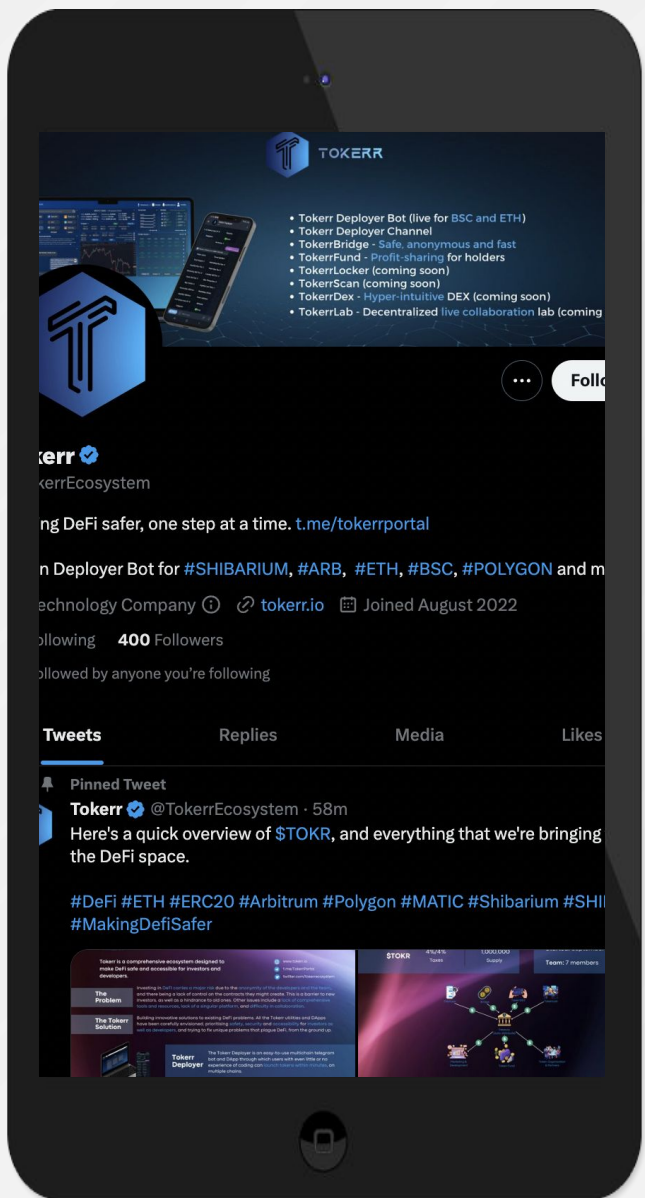
SOCIAL MEDIA

& ONLINE PRESENCE



ANALYSIS

Project's social media pages are active.



Twitter

@tokerrecosystem

- 396 followers
- Posts frequently
- Active



Discord

<https://discord.com/in/vite/KZA6NNSrzc>

- 25 members
- Few active members



Telegram

@tokerrportal

- 896 members
- Active members
- Active mods



Medium

- Not available



SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 400 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE



[SPYWOLF.CO](https://spywolf.co)



[@SPYWOLFNETWORK](https://t.me/SPYWOLFNETWORK)



[@SPYWOLFNETWORK](https://twitter.com/SPYWOLFNETWORK)



Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.